REMARKS

This response is submitted in reply to the Office Action dated March 9, 2005. Claims 1-23 are pending in the patent application. Claims 1, 5, 13, 14 and 21-23 have been amended. No new matter has been added by any of the amendments made herein.

In the Office Action, the specification, figures and claims 1 and 13 were objected to. Claims 1-23 were rejected under 35 U.S.C. § 102(e). Applicants respectfully submit, for at least the reasons set forth below, that the objections and rejections have been overcome or are improper. Accordingly, Applicants respectfully request reconsideration of the patentability of Claims 1-23.

The specification was objected to because of an informality. Specifically, the Office Action states that the disclosure is not consistent with the drawing. For example, figure 7 shows "next authentication request" as step 6; "receive digital signature from server" at step 7 . . .. Applicants respectfully disagree. In Applicants' Response to Office Action dated September 15, 2004, filed on December 15, 2004, ("Prior Response"), Applicants amended the Specification beginning at page 10 line 3 to read, "When the encryption module 23 receives the digital signature sheet from the security server 6 (in step SP6), the CPU 10 of the user terminal 4 sends it to the WWW browser 10 through PKCS#11-24 (in step SP7). Then, the CPU 10 sends the received digital signature sheet to the WWW server 3 as the acknowledgement of the authentication request (in step SP8)." See, Prior Response, page 2. Accordingly, Applicants respectfully request that this objection is improper and should be withdrawn.

Figures 6 and 7 were objected to as failing to comply with 37 CFR § 1.84(p)(5) because the reference sign "SP6" is not mentioned in the specification. Applicants respectfully disagree. As detailed above, amended replacement Figures 6 and 7 were submitted in Applicants' Prior Response. Applicants hereby enclose a copy of the postcard indicating the submission of Figures 6 and 7 with the Patent Office's acknowledgement of such. The previously submitted amendments to the specification and drawings more clearly indicated proper consistency between the specification and drawings. However, in an effort to fully cooperate and to further the prosecution, Applicants hereby include, as an attachment to this Amendment, copies of the previously submitted amended drawings. Accordingly, Applicants respectfully request that this objection is improper and should be withdrawn.

Claims 1 and 13 were objected to for informalities. For example, in claim 1, the number "10" should be deleted and in claim 13, the number "30" should be deleted. Accordingly, Applicants have amended claims 1 and 13 to delete the numbers "10" and "30" respectively. Applicants respectively request that the objections to claims 1 and 13 are overcome and the objections should be withdrawn.

Claims 1-23 were rejected under 35 U.S.C. § 102 as being anticipated by U.S. Patent No. 6,694,436 to Audebert ("Audebert"). Applicants respectfully disagree with and traverse this rejection because Audebert fails to properly anticipate the present invention.

Of the rejected claims, 1, 5, 13-14 and 21-23 are the sole independent claims. Claims 1, 5, 13-14 and 21-23 have been amended as fully supported in the Specification, for example, at page 6, lines 19-27. Independent claim 1 is directed to a user authentication system, that includes a data holding medium for holding a common key unique to a user, used in a common-key encryption method, wherein the data holding medium includes a radio function for sending information read from the data holding medium by radio, and writing information to the data holding medium by radio; an authentication apparatus for holding the common key used in the common-key encryption method and a private key used in a public-key encryption method, each unique to the user; and an information processing apparatus connected to the authentication apparatus in an always-communicable manner and provided with a function for performing authentication by the public-key encryption method; wherein the authentication apparatus performs authentication by using the common key held by the data holding medium and the common key held by the authentication apparatus, in response to a user authentication request sent from the information processing apparatus, and, only when the user has been authenticated, performs processing for making the information processing apparatus authenticate the user by using the private key corresponding to the user.

Independent claim 5 relates to a user authentication method for a user who carries a data holding apparatus for holding a common key used in a common-key encryption method, the method includes the steps of: reading the common key from the data holding apparatus by radio; authenticating the user by the common-key encryption method by using the common key held by the data holding apparatus of the user in response to a user authentication request; and

performing, only when the user has been authenticated, processing for authenticating the user by a public-key encryption method.

Independent claim 13 relates to an authentication method, that includes the steps of: holding a common key used in a common-key encryption method and a private key used in a public-key encryption method, for each user; sending the common key and the private key read from each user by radio; authenticating, in response to a user authentication request sent from an external information processing apparatus, the user by using the held common key for the user and a common key used in the common-key encryption method which the user has and is held by a data holding apparatus; and performing, only when the user has been authenticated in the authentication step, processing for making the information processing apparatus authenticate the user by the public-key encryption method by using the private key corresponding to the user.

Independent claim 14 is directed to an authentication apparatus, that includes: a holder for holding a common key used in a common-key encryption method and a private key used in a public-key encryption method, for each user; the holder for holding the common key and the private key including a radio function for sending information read from the holder by radio, and writing information to the holder by radio; and an authenticating device for, in response to a user authentication request sent from an external information processing apparatus, authenticating the user by using the common key for the user held by the holder and a common key used in the common-key encryption method for the user held by a data holding medium of the user, and for, only when the user has been authenticated, performing processing for making the information processing apparatus authenticate the user by the public-key encryption method by using the private key corresponding to the user.

Independent claim 21 is directed to a user authentication system, wherein a data holding medium for holding a common key unique to a user, used in a common key encryption method, that includes: a server for sending an authentication request to perform a service to the user; and an authentication apparatus that includes, a holding means for holding the common key used in a common-key encryption method for authentication between a data holding medium held by the user and the authentication apparatus, said holding means holding a private key used in a public-key encryption method to the authentication between the data holding medium and the server; the holding means including a radio function for sending information read from the holding

means by radio, and writing information to the holding means by radio; and means for authenticating the data holding medium by using the common key for the user held by the holding means and a common key used in the common-key encryption method for the user held by the data holding medium in response to the authentication request sent from the server, said authenticating means performing a processing for authentication between the data holding medium and the server by using the private key corresponding to the user when the data holding medium has been authenticated by using the common keys.

Independent claim 22 relates to an authentication method between a data holding medium and a server by an authentication apparatus, said data holding medium holding a common key unique to a user, used in a common-key encryption method, wherein said authentication apparatus holds the common key and a private key used in a public-key encryption method, the authentication method including the steps of: sending the common key and the private key from the data holding medium to the authentication apparatus by radio and writing information received from the authentication apparatus to the data holding medium by radio; authenticating, in response to an authentication request sent form the server to perform a service to the user, the data holding medium by using the common key for the user held by the authentication apparatus and a common key used in the common-key encryption method held by the data holding medium; and performing a processing for authentication between the data holding medium and the server by using the private key corresponding to the user when the data holding medium has been authenticated by using the common keys.

Independent claim 23 is directed to an authentication apparatus, including: a holding means for holding a common key used in a common-key encryption method for authentication between a data holding medium held by the user and the authentication apparatus, said holding means holding a private key used in a public-key encryption method for authentication between the data holding medium and a server; the data holding medium including a radio function for sending information read from the data holding medium to the authentication apparatus by radio, and writing information received from the authentication apparatus to the data holding medium by radio; and means for authenticating the data holding medium by using the common key for the user held by the holding means and a common key used in the common-key encryption method for the user held by the data holding medium in response to the authentication request

sent from the server, said authenticating means performing a processing for authentication between the data holding medium and the server by using the private key corresponding to the user when the data holding medium has been authenticated by using the common keys.

On the contrary, Audebert is directed to a terminal and system for performing secure electronic transactions. Audebert discloses that the microcircuit card and the integrated circuit card reader are connected to the computer via a variety of interfaces, such as PCMCI. See, Audebert, Col. 26, ln. 50-65. Further, Audebert teaches that to enhance further the security of the transaction system in accordance with the invention, a conventional authentication process can be used for authentication by the terminal module **1, 101** of the microcircuit card used. The authentication process prevents the user's personal identification number (PIN), entered by the latter into the module **1, 101** via the keyboard **5** to execute a secured transaction, from being captured by a counterfeit card substituted by a hacker for the user's authentic card and subsequently recovered by the hacker to read the PIN off the counterfeit card. See, Audebert, Col. 26, ln. 27-44. Cleary, the authentication process in Audebert does not disclose to one skilled in the art that sending or receiving of such authentication information by radio would be possible by the terminal and system for performing secure electronic transactions. In fact, nowhere in Audebert is it even disclosed or suggested that the common key or private key may be transmitted by radio, or that the computer can send or receive same by radio. As discussed above, Audebert merely provides that the integrated circuit card reader is connected via a variety of interfaces, such as PCMCI, which clearly teaches away from such means as radio. Therefore, Applicants believe that Audebert is distinguishable from the claimed invention.

Accordingly, Applicants respectfully request that the anticipation rejection with respect to claims 1-23 be reconsidered, and, thus, the rejection be withdrawn based on at least the reasons discussed above.

For the foregoing reasons, Applicants respectfully submit that the present application is in condition for allowance and earnestly solicit reconsideration of same.

Respectfully submitted,

BELL, BOYD & LLOYD LLC

BY _____

Thomas C. Basso
Reg. No. 46,541
P.O. Box 1135
Chicago, Illinois 60690-1135
Phone: (312) 807-4310

Dated: May 6, 2005